PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00

A2

(11) International Publication Number: WO 99/56194

(43) International Publication Date: 4 November 1999 (04.11.99)

(21) International Application Number: PCT/US99/09441

(22) International Filing Date: 29 April 1999 (29.04.99)

(30) Priority Data:

60/083,714	30 April 1998 (30.04.98)	US
09/283,540	1 April 1999 (01.04.99)	US

(81) Designated States: CN, IN, JP, RU, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published

Without international search report and to be republished upon receipt of that report.

(71) Applicant: EC CUBED, INC. [US/US]; Suite 310, 15 River Road, Wilton, CT 06897 (US).

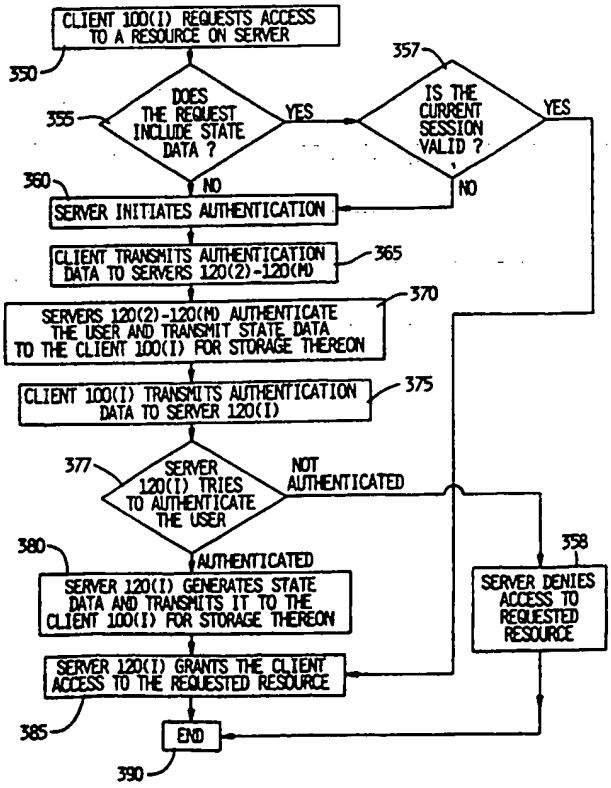
(72) Inventors: BARTOLOMEOS, Ephrem; 86 Grove Street #B6, Stamford, CT 06901 (US). WAINGANKAR, Pramod; 9 Hamilton Avenue, Norwalk, CT 06897 (US). RENGARAJAN, Vasu; 10 Clapboard Ridge Road #42J, Danbury, CT 06811 (US). HOQUE, Faisal; 96 Glenbrook Road #38, Stamford, CT 06902 (US).

(74) Agent: COHEN, Neil, G.; Cummings & Lockwood, Four Stamford Plaza, Stamford, CT 06904 (US).

(54) Title: SYSTEM AND METHOD FOR AUTHENTICATING A USER TO MULTIPLE SERVERS IN A DISTRIBUTED COMPUTING NETWORK

(57) Abstract

A method and system for a server to facilitate authentication of a user of a client by a second server is disclosed. According to a disclosed method, the server, the second server, and the client communicate in a distributed computing network and the server and the second server store a plurality of restricted resources. The method includes the steps of storing data identifying the second server in the server, receiving a request to access one of the plurality of restricted resources from the client, and transmitting the data identifying the second server to the client so that the user of the client can be authenticated by the second server.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SYSTEM AND METHOD FOR AUTHENTICATING A USER TO MULTIPLE SERVERS IN A DISTRIBUTED COMPUTING NETWORK

CROSS-REFERENCE TO RELATED APPLICATION

This application claims priority to United States Provisional Patent Application Serial Number 60/083,714, filed April 30, 1998, the disclosure of which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

The Internet is a distributed computer network that permits multiple servers and clients to communicate with each other. Servers and clients communicate according to a predefined communications protocol. In the case of Internet communications using the World Wide Web ("Web"), the protocol is Hypertext Transport Protocol ("HTTP") running over a Transmission Control Protocol/Internetworking Protocol ("TCP/IP"). The underlying TCP/IP protocol requires that each server and client have a unique code associated with it that identifies the server and client, respectively, on the network. The unique code is known as an Internet Protocol ("IP") address.

A server is an application program running on a computer for making data, files, documents, web pages, and/or other resources (collectively, "resources") stored within the computer available to clients requesting access to such resources. As is well known, some of the resources may contain sensitive or restricted information. Typically, these restricted resources are only provided to users of a client that are authenticated by the server storing such resources.

When a client requests access to a restricted resource from a server, the server initiates an authentication process. According to a typical authentication process, upon receiving a request to access a restricted resource, the server prompts the user of the client requesting access to provide authentication data, for example, an identification code ("User ID") and a password, back to the server. A user operating the client responds to the prompt by entering his or her authentication data and causes this data to be transmitted to the server.

When the server receives the authentication data, it determines whether such data matches data stored in a record for the user in an account database residing on the server. The server grants the user access to the restricted resource if the authentication data matches the data stored in the record and the user has been given access privileges to the restricted resource. When access is granted, the server transmits the requested restricted resource to the client, which may display it to the user on a monitor. If the authentication data does not match the data stored in the record, then the server denies the user access to the restricted resource. United States Patent No. 5,708,780 to Levergood et al., the disclosure of which is incorporated herein by reference, describes a typical authentication process in more detail.

When a server successfully authenticates a user of a client, it is common to store state data (e.g., in the form of a cookie) on the client. Such state data typically includes data that identifies the client, data that identifies the server, data that identifies the session (e.g., the restricted resource(s) accessed, the time of such access, the time that the user was authenticated) and the authentication data of the user (e.g., a User ID and password). In this way, as is well known, when the client attempts to access another restricted resource on the server at a later time, the client transmits a request for access to the restricted resource which includes the state data. Because the server receives the state data, it determines that the user of the client has already been authenticated, which eliminates the need for repetition of the authentication process.

It is well known for enterprises to use servers to provide numerous unrestricted and restricted resources to users. The data representing the resources is often very large, and in such cases, it is distributed across multiple servers that communicate in a distributed computing network. For example, consider a scenario in which the data resides on two or more servers connected via a distributed computer network (e.g., the Internet). If a client attempts to access a restricted resource stored on one of the servers, then that server will authenticate the user prior to providing access to the restricted resource. If the authentication is successful, then the server will permit the user to access the requested resource.

However, when the client attempts to access a restricted resource residing on other servers in the network, then the authentication process is repeated again by the other servers. Thus, a user is authenticated by each server from which he tries to access a restricted resource. As most users have experienced, this quickly becomes a repetitive process that is quite tedious and burdensome.

In view of the above, a substantial need exists for a method and system in which a user of a client provides authentication data to only one server in a distributed computing network, yet can be authenticated by other servers in the distributed computing network.

BRIEF DESCRIPTION OF THE DRAWINGS

Representative embodiments of the present invention will be described with reference to the following figures:

FIG. 1 is an overview of an environment in which an embodiment of the present invention may be used.

FIG. 2 is a block diagram of an embodiment of a server within a distributed computing network.

FIG. 3 is a flowchart illustrating an embodiment of a process for authenticating a user of a client to multiple servers within a distributed computing network.

FIGS. 4 is a flowchart illustrating an alternate embodiment of a process for authenticating a user of a client to multiple servers within a distributed computing network.

SUMMARY OF THE INVENTION

One aspect of the present invention is directed to a method for a server to facilitate authentication of a user of a client by a second server. The server, the second server, and the client communicate in a distributed computing network. The server and the second server store a plurality of restricted resources. The method includes the steps of storing data identifying the second server in the server, receiving a request to access one of the plurality of restricted resources from the client, and transmitting the data identifying the second server to the client so that the user of the client can be authenticated by the second server.

Another aspect of the present invention is directed toward a server for facilitating authentication of a user of a client by a second server. The server, the second server, and the client communicate in a distributed computing network. The server and the second server store a plurality of restricted resources. The server includes a memory storing data identifying the second server and a processor in communication with the memory. The processor is operative to receive a request to access one of the plurality of restricted resources from the client and transmit the data identifying the second server to the client so that the user of the client can be authenticated by the second server.

Yet another aspect of the present invention is directed toward a method for a server to facilitate authentication of a user of a client by a second server. The server, the second server, and the client communicate in a distributed computing network. The

method includes the steps of storing first data identifying the user and data identifying the second server, receiving second data identifying the user, determining whether the second data corresponds to the first data, and when the second data corresponds to the first data, transmitting third data identifying the user to the second server based on the data identifying the second server so that the second server can authenticate the user.

Still another aspect of the present invention is directed to a system for facilitating authentication of a user of a client by a first server and a second server. The server, the second server, and the client communicate in a distributed computing network. The first server and the second server store a plurality of restricted resources. The system includes a first memory associated with the first server storing data identifying the second server and first data identifying the user, and a first processor associated with the first server in communication with the first memory. The first processor is operative to receive a request to access one of the plurality of restricted resources from the client and transmit the data identifying the second server to the client. The system further includes a second memory associated with the second server storing second data identifying the user and a second processor associated with the second server in communication with the second memory. The second processor is programmed to receive third data identifying the user from the client, determine whether the second data corresponds to the third data, and authenticate the user when the second data corresponds the third data.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Reference is now made to the accompanying Figures for the purpose of describing, in detail, the preferred embodiments of the present invention. The Figures and accompanying detailed description are provided as examples of the invention and are not intended to limit the scope of the claims appended hereto.

As will become more apparent from the following description, the present invention provides a novel and unique method and system in which a user of a client

submits authentication data to one server in a distributed computing network in order to access a restricted resource, yet the user is also authenticated by other servers in the network. In so doing, the method and system serves to eliminate the repetitive, tedious, and burdensome requirement that the user provide authentication data to each server in a distributed computing network from which it requests access to a restricted resource.

FIG. 1 shows an overview of an environment in which an embodiment of the present invention may be used. The environment includes a network 110, clients 100(1)-100(N), and servers 120(1)-120(M). The variables "N" and "M" represent the numbers of clients and servers, respectively within the environment. The variables "M" is greater or equal to two and the variable "N" is at least one.

Network 110 is a distributed computing network that enables communication between clients 100 and servers 120. For example, network 110 may be the Internet, an intranet, a local area network (LAN), or a wide area network (WAN). In the exemplary embodiments described hereafter, network 110 is the Internet.

Clients 100 are devices that are able to communicate with at least two of servers 120 via network 110. For example, a client 100 may be a conventional desktop personal computer or a workstation running software that enables communication with servers 120. Alternatively, a client 100 may be a cellular telephone, telephone, pager, and/or other personal-type device running appropriate software that enables communication with servers 120. Clients 100(1)-100(N) communicate with network 110 via communication channels 160(1)-160(N), respectively. The communication channels 160, whether wired or wireless, are well known and therefore are not further described here.

As is well known, each client 100 has a unique network address. In an embodiment in which network 110 is the Internet, the unique network address for each client 100 is an IP address.

Each client 100 has one or more users associated with it. A user may use a client 100 to access resources stored on one or more of servers 120.

Each client 100 includes a memory that stores software that may be used for accessing resources residing on servers 120. In one embodiment, the software is a Web browser that uses the HTTP communication protocol to communicate with servers 120 in order to access resources stored thereon.

As is well known, Web browser software is capable of transmitting requests to access resources ("access requests") that are stored on servers 120 and storing state data (e.g., in the form of a cookie) on a client 100 on which it is running. Two well known Web browsers are Netscape's Navigator and Microsoft's Internet Explorer. An access request includes data identifying the requested resource, and may include state data stored on the client 100, if any.

Servers 120 are devices that are able to communicate with clients 100 via network 110. Servers 120(1)-120(M) communicate with network 110 via communication channels 170(1)-170(M), respectively. The communication channels 170, whether wired or wireless, are well known and therefore are not further described here. As is well known, each server 120 has a unique network address, for example, an IP address when the network is the Internet. In the preferred embodiment, servers 120 are Web (HTTP) servers.

Servers 120 store resources, which are accessed by clients 100 over network 110. For example, resources include any data, files, documents, web pages, and/or other resources residing on servers 120. In the description that follows, a resource will be referred to as "restricted" if a user of a client must be authenticated before such user is permitted access to the resource. Alternatively, a resource will be referred to as "unrestricted" if a user of a client need not be authenticated before such user is permitted access to the resource.

Servers 120 also store other software and databases as will be described in more detail below. One such software program is for authenticating users of clients 100 to determine whether they should be granted access to a restricted resource residing on servers 120.

FIG. 2 depicts an exemplary embodiment of a server 120. This exemplary server 120 includes a memory 127 and at least one processor 125 in communication with memory 127. In a preferred embodiment, each server 120 shares a similar architecture.

Memory 127 typically includes one or more machine readable media. Such machine readable media include, as is well known in the art; an appropriate combination of magnetic, semiconductor and optical media such as a hard disk, optical disk, floppy disk, tape, RAM, ROM, and/or WORM.

Memory 127 includes a user database 127A, a server database 127B, a session database 127C, and program code 127D. These are now each described in more detail.

User database 127A stores data identifying users of clients 100. For the purpose of simplicity, the description that follows is provided with respect to one such user of a client 100.

In one embodiment, user database 127A stores authentication data in the form of an alphanumeric user identifier ("User ID") and a password for each user. In other embodiments, user database 127A may also include data identifying resources to which a user has access and the last time that the user accessed such resources.

Server database 127B stores data that identifies servers 120 in the network 110. In one embodiment, server database 127B includes a network address (e.g., an IP address) for each server 120. In an alternate embodiment, server database 127B includes a Uniform Resource Locator (URL) for each such server. In still another embodiment, server database 127B may include both a network address and a URL for servers 120.

Session database 127C stores data identifying resources accessed by clients 100. In one embodiment, session database 127C includes data that identifies a resource accessed by a client 100 and the time that the resource was accessed. In other embodiments, session database 127C of a server 120 may also store a time that the user of the client 100 was authenticated by the server 120. As is well known in the art, the data stored in session database 127C is transient -- that is, it is removed by the server at predetermined times.

Program code 127D includes software for controlling processor 125 in accordance with the flowcharts of FIGS. 3 and 4.

FIG. 3 is a flow chart illustrating an embodiment of a process for authenticating a user of a client 100 to multiple servers 120 within network 110.

At step 350, a user of a client 100 causes the client 100 to transmit a request to one of servers 120 for access to a restricted resource residing thereon. For the purpose of simplicity, in the following description, the client 100(1) transmits the access request to server 120(1).

In this described embodiment, the access request is transmitted over the Internet and includes data identifying the requested restricted resource and data identifying the client. It may also include the version of the browser software that the client 100(1) is running and the version of the HTTP protocol that the client 100(1) is running.

Additionally, if the user of the client 100(1) has been authenticated previously, then the access request will also include state data that has been stored on the client 100(1). In one embodiment, the state data includes data that identifies the client 100(1) (e.g., IP address of the client 100(1)), data that identifies the server 120(1) (e.g., an IP address of the server 120(1)), data that identifies the session (e.g., the resources accessed, the time of such accesses, the time that the user was authenticated) and authentication data (e.g., a User ID and password). The state data may also include an

expiration period of the state data to prevent unnecessary use of the client's 100(1) storage capacity.

At step 355, the server 120(1) determines if the access request of the user of the client 100(1) includes state data. This is done in a well known manner. If the access request transmitted by the client 100(1) is determined to include the state data, the server 120(1) proceeds to step 357. If the access request is determined not to include the state data, then the server 120(1) proceeds to step 360.

At step 357, the server 120(1) determines if the session is valid. To accomplish this, the server determines if the authentication data and session data included in the state data have corresponding matches in the user database 127A and session database 127C, respectively, of server 120(1). If corresponding matches are found, then the session is valid for the client 100(1), and the server 120(1) proceeds to step 385. If corresponding matches are not found, then the session is not valid for the client 100(1), and the server 120(1) proceeds to step 360. In one embodiment, at step 357, if the session is valid, the server 120(1) updates the state data on the client 100(1) and the data identifying the session in its session database 127C.

At step 360, the server 120(1) transmits an authentication request that prompts the user of the client 100(1) for authentication data. Server 120(1) also transmits data identifying the servers 120 on the network 110 to the client 100(1). In one embodiment, the data identifying the servers 120 is the IP addresses of the servers 120 and the authentication data is a User ID and a password. The authentication request transmitted by the server 120(1) contains code for the client 100(1) to execute. This code may be in JavaScript or VBScript standard format, or some other format.

At step 365, the client 100(1) transmits the user's authentication data to other servers 120(2)-120(M) identified by the data received at step 360 from server 120(1). Thus, in this example, the client 100(1) executes the code contained in the authentication request (received at step 360) so as to initiate an authentication process

with the servers 120(2)-120(M) on the network 110. For the purpose of simplicity, the following description is set forth for server 120(2), which receives an authentication request from the client 100(1). The other servers 120(3)-120(M) would authenticate the user in a similar manner. In this authentication process, client 100(1) submits the user's authentication data to server 120(2) in the form of a User ID and a password.

At step 370, server 120(2) authenticates the user of the client 100(1). The specific type of authentication processes is not critical to the present invention, as long as it enables a server 120 to verify that the user of the client 100(1) is authorized to receive a requested restricted resource. In one embodiment, the authentication process includes server 120(2) comparing the user's authentication data transmitted by client 100(1) at step 365 to the data stored in the user database 127A of server 120(2).

For example, if the transmitted authentication data is a User ID and a password, then server 120(2) compares such User ID and password to the User IDs and passwords stored in user database 127A of the server 120(2). If the authentication data has a corresponding entry in the data stored in the user database 127A, then the server 120(2) generates state data (e.g., in the form of a cookie). The server 120(2) transmits the state data (as described above) to the client 100(1) for storage thereon. Server 120(2) also creates and stores corresponding session data in its session database 127C.

Client 100(1) continues transmitting authentication requests to each of the other servers 120(3)-120(M) identified by the data provided to the client 100(1) by server 120(1) at step 360 so as to be authenticated by those servers. In one embodiment, if a server 120(2)-120(M) does not respond to an authentication request of client 100(1) within a predefined time period, then a time out mechanism will trigger the process to continue without authentication occurring at that server. According to an additional feature, if an authentication attempt fails at a server 120(2)-120(M), then client 100(1) will receive notice and proceed to continue the process with another server until each

server identified by the data received at step 360 is exhausted. As is readily apparent, not all servers 120(1)-120(M) need to successfully authenticate the user of client 100(1).

At step 375, client 100(1) transmits the user's authentication data to server 120(1) via the network 110.

At step 377, server 120(1) authenticates the user as described above at step 370. If the transmitted authentication data has a match in the user database 127A, then processing proceeds to step 380. If the transmitted authentication data does not have a match in the user database 127A, then the user is not valid, server 120(1) denies the user access to the requested resource at step 358, and the process ends at step 390. In this latter case, the user would be denied access to a restricted resource on server 120(1), yet might be given access to other restricted resources residing on servers 120(2)-120(M).

At step 380, server 120(1) generates state data (e.g., in the form of a cookie) and transmits it to the client 100(1) for storage. Server 120(1) also creates and stores corresponding session data in its session database 127C.

At step 385, server 120(1) grants the user access to the requested restricted resource. In one embodiment, the restricted resource is a data file that the server 120(1) transmits to the client 100(1) via the network 110. At step 390, the process ends.

After a user of the client 100(1) is authenticated by one or more servers 120, the user's requests for access to other restricted resources on servers 120 will include state data. When a server 120 determines that an access request includes state data, then the server 120 will not need to authenticate the user of the client 100(1). Thus, the repetitive, tedious and burdensome authentication process need not be repeated by the user, and servers 120 can immediately grant access to the restricted resource.

FIG. 4 is a flow chart illustrating an alternative process for authenticating a user of a client 100 to multiple servers 120 within a distributed computing network 110.

Steps 405, 410, 412 and 415 are executed as described above in FIG. 3 at steps 350, 355, 357 and 360, respectively.

However, at step 412, if the session is valid for the client 100(1), then the server 120(1) updates the state data on the client 100(1) and the data identifying the session in its session database 127C in memory 127 and proceeds to step 425.

At step 415, server 120(1) prompts the user of the client 100(1) for authentication data as described above in FIG. 3 at step 360. At step 417, the client 100(1) transmits the user's authentication data to server 120(1).

At step 420, server 120(1) determines whether the transmitted authentication data is sufficient to authenticate the user as described above in FIG. 3 at step 377. If the user is not authenticated, server 120(1) denies access to the requested restricted resource, server 120(1) denies the user access to the requested resource at step 421, and the process ends at step 475. If the user is authenticated, the server 120(1) proceeds to step 425.

At step 425, the server 120(1) generates state data (e.g., in the form of a cookie) and transmits the state data to the client 100(1) for storage.

At step 430, server 120(1) grants the user access to the requested restricted resource as described above in FIG. 3 at step 385. At step 430, processor 125 of server 120(1) also generates data identifying the session and stores it as part of session database 127C.

At step 460, server 120(1) retrieves data identifying servers 120(2)-120(M). In one embodiment, server 120(1) retrieves the IP addresses of servers 120(2)-120(M) that are stored as part of server database 127B in memory 127.

At step 465, server 120(1) transmits the authentication data transmitted by the user and data in session database 127C to the other servers 120(2)-120(M). In one embodiment, the server 120(1) transmits the authentication data of the user of the client 100(1) and session data generated at step 430.

At step 470, each server 120(2)-120(M) authenticates the user of the client 100(1) as described above in FIG. 3 at step 370.

If the authentication is successful, either directly or via server 120(1), each of the servers 120 transmits corresponding state data to the client 100(1). The client 100(1) stores the state data, which will be sent to a server 120(2)-120(M) when the user makes a request to access a restricted resource residing thereon. At step 475, the process ends. The inventors of course realize that the current HTTP protocol does not support a server initiating contact with a client; however, future modified versions of the HTTP protocol and/or other protocols may support such contact.

As is readily apparent, the invention fulfills the substantial need which exists for a method and system wherein a user of a client is required to provide authentication data to one server in a distributed computing network, yet can be authenticated by multiple servers in the distributed computing network. As a result, the present invention eliminates the repetitive, tedious and burdensome task of the prior art user authentication process.

Although the particular embodiments shown and described above are useful in many applications relating to the arts to which the present invention pertains, further modifications of the present invention herein disclosed will occur to persons skilled in the art. All such modifications are deemed to be within the scope and spirit of the present invention.

WE CLAIM:

1. A method for a server to facilitate authentication of a user of a client by a second server, wherein the server, the second server, and the client communicate in a distributed computing network, wherein the server and the second server store a plurality of restricted resources, and wherein the method comprises:

(a) storing data identifying the second server in the server;

(b) receiving a request to access one of the plurality of restricted resources from the client; and

(c) transmitting the data identifying the second server to the client so that the user of the client can be authenticated by the second server.

2. The method of Claim 1, wherein the plurality of restricted resources comprise files, documents, and web pages.

3. The method of Claim 1, wherein the distributed computing network is the Internet, and wherein the data identifying the second server is selected from the group comprising an IP address of the second server and a uniform resource locator of the second server.

4. The method of Claim 1, wherein the request to access one of the plurality of restricted resources comprises data identifying the restricted resource.

5. The method of Claim 1, further comprising the step of transmitting data to the client that prompts the user to provide authentication data relating to the user.

6. The method of Claim 5, further comprising the steps of receiving the authentication data relating to the user and authenticating the user based on the authentication data.

7. The method of Claim 6, wherein the authentication data comprises a user ID and a password of the user.

8. The method of Claim 6, further comprising the step of generating state data when the user has been authenticated.

9. The method of Claim 8, further comprising the step of transmitting the state data to the client for storage thereon.

10. The method of Claim 9, further comprising the step of transmitting the requested restricted resource to the client when the user has been authenticated.

11. A server for facilitating authentication of a user of a client by a second server, wherein the server, the second server, and the client communicate in a distributed computing network, wherein the server and the second server store a plurality of restricted resources, and wherein the server comprises:

(a) a memory storing data identifying the second server; and

(b) a processor in communication with the memory, wherein the processor is operative to

(i) receive a request to access one of the plurality of restricted resources from the client; and

(ii) transmit the data identifying the second server to the client so that the user of the client can be authenticated by the second server.

12. The server of Claim 11, wherein the plurality of restricted resources comprise files, documents, and web pages.

13. The server of Claim 11, wherein the distributed computing network is the Internet and wherein the data identifying the second server is selected from the group comprising an IP address of the second server and a uniform resource locator of the second server.

14. The server of Claim 11, wherein the request to access one of the plurality of restricted resources comprises data identifying the restricted resource.

15. The server of Claim 11, wherein the processor is further operative to transmit data to the client that prompts the user to provide authentication data relating to the user.

16. The server of Claim 15, wherein the processor is further operative to receive the authentication data relating to the user and authenticate the user based on the authentication data.

17. The server of Claim 16, wherein the authentication data comprises a user ID and a password of the user.

18. The server of Claim 16, wherein the processor is further operative to generate state data when the user has been authenticated.

19. The server of Claim 18, wherein the processor is further operative to transmit the state data to the client for storage thereon.

20. The server of Claim 19, wherein the processor is further operative to transmit the requested restricted resource to the client when the user has been authenticated.

21. A method for a server to facilitate authentication of a user of a client by a second server, wherein the server, the second server, and the client communicate in a distributed computing network, and wherein the method comprises:

(a) storing first data identifying the user and data identifying the second server;

(b) receiving second data identifying the user;

(c) determining whether the second data corresponds to the first data; and

(d) when the second data corresponds to the first data, transmitting third data identifying the user to the second server based on the data identifying the second server so that the second server can authenticate the user.

22. The method of Claim 21, wherein the server and the second server store a plurality of restricted resources, and further comprising the step of receiving a request to access one of the plurality of restricted resources from the client.

23. The method of Claim 22, further comprising the step of transmitting data to the client that prompts the user to provide authentication data relating to the user.

24. The method of Claim 23, further comprising the steps of receiving the authentication data relating to the user and authenticating the user based on the authentication data.

25. The method of Claim 23, wherein the authentication data comprises a user ID and a password of the user.

26. The method of Claim 24, further comprising the step of generating state data when the user has been authenticated.

27. The method of Claim 26, further comprising the step of transmitting the state data to the client for storage thereon.

28. The method of Claim 27, further comprising the step of transmitting the one of the plurality of restricted resources to the client when the user has been authenticated.

29. A system for facilitating authentication of a user of a client by a first server and a second server, wherein the first server, the second server, and the client communicate in a distributed computing network, wherein the first server and the second server store a plurality of restricted resources, and wherein the system comprises:

(a) a first memory associated with the first server storing data identifying the second server and first data identifying the user; and

(b) a first processor associated with the first server in communication with the first memory, wherein the first processor is operative to

(i) receive a request to access one of the plurality of restricted resources from the client; and

(ii) transmit the data identifying the second server to the client;

(c) a second memory associated with the second server storing second data identifying the user; and

(d) a second processor associated with the second server in communication with the second memory, wherein the second processor is programmed to

(i) receive third data identifying the user from the client;

(ii) determine whether the second data corresponds to the third data; and

(ii) authenticate the user when the second data corresponds the third data.

30. The system of Claim 29, wherein the plurality of restricted resources comprise files, documents, and web pages.

31. The system of Claim 29, wherein the distributed computing network is the Internet and wherein the data identifying the second server is selected from the group comprising an IP address of the second server and a uniform resource locator of the second server.

32. The system of Claim 29, wherein the request to access one of the plurality of restricted resources comprises data identifying the restricted resource.

33. The system of Claim 29, wherein the first, second, and third data identifying the user comprises a user ID and a password of the user.

34. The system of Claim 29, wherein the first processor is further operative to transmit data to the client that prompts the user to provide authentication data relating to the user.

35. The system of Claim 34, wherein the first processor is further operative to receive the authentication data relating to the user and authenticate the user based on the authentication data.

36. The system of Claim 35, wherein the first processor is further operative to generate state data when the user has been authenticated.

37. The system of Claim 36, wherein the first processor is further operative to transmit the state data to the client for storage thereon.

38. The system of Claim 37, wherein the first processor is further operative to transmit the one of the plurality of requested restricted resources to the client when the user has been authenticated by the first server.

39. The system of Claim 37, wherein the second processor is further operative to transmit the one of the plurality of the restricted resources to the client when the user has been authenticated by the second server.

40. The method of Claim 8, wherein the state data comprises data identifying the client, data identifying the server, data identifying a session between the client and the server, and the authentication data.

41. The server of Claim 18, wherein the state data comprises data identifying the client, data identifying the server, data identifying a session between the client and the server, and the authentication data.

42. The method of Claim 26, wherein the state data comprises data identifying the client, data identifying the server, data identifying a session between the client and the server, and the authentication data.

43. The system of Claim 36, wherein the state data comprises data identifying the client, data identifying the server, data identifying a session between the client and the server, and the authentication data.

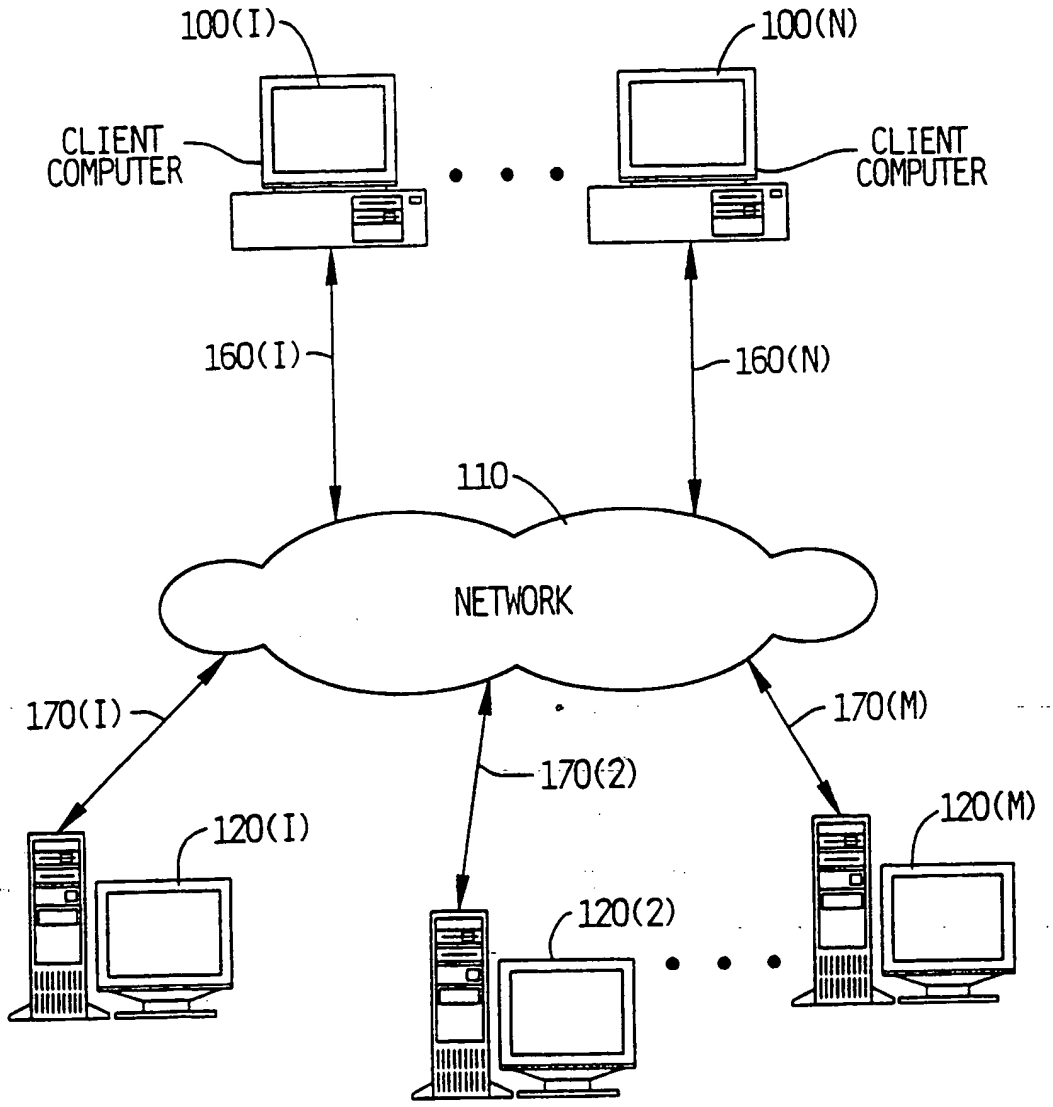

100(I)
100(N)
CLIENT COMPUTER
CLIENT COMPUTER
160(I)
160(N)
110
NETWORK
170(I)
170(2)
170(M)
120(I)
120(2)
120(M)

FIG_1

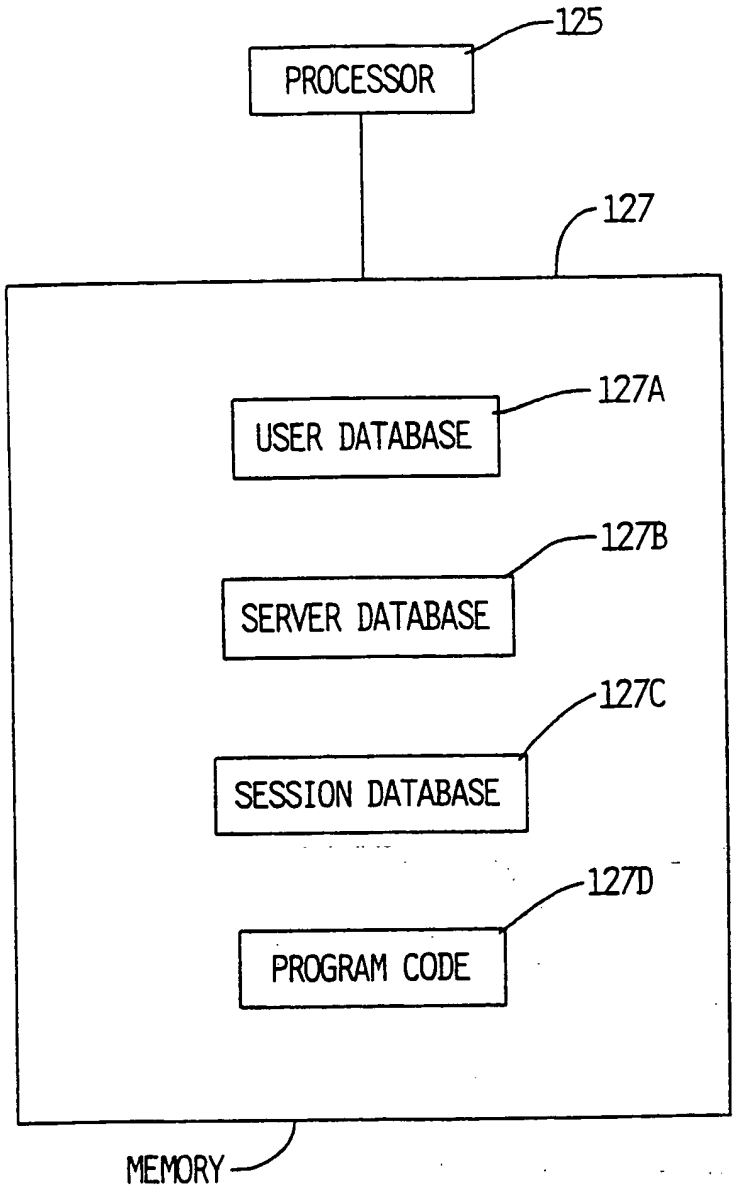

125
PROCESSOR
127
127A
USER DATABASE
127B
SERVER DATABASE
127C
SESSION DATABASE
127D
PROGRAM CODE
MEMORY

FIG_2

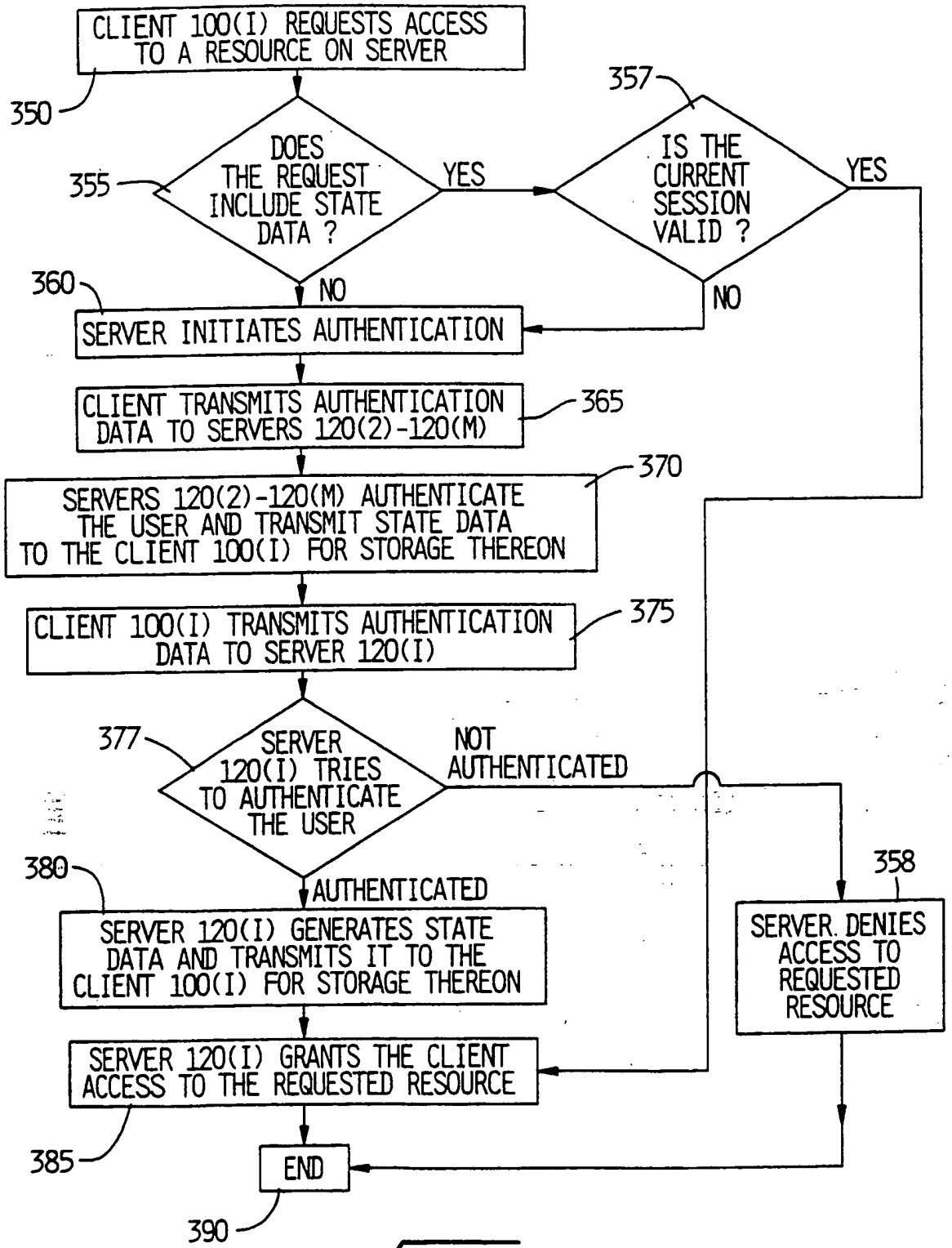
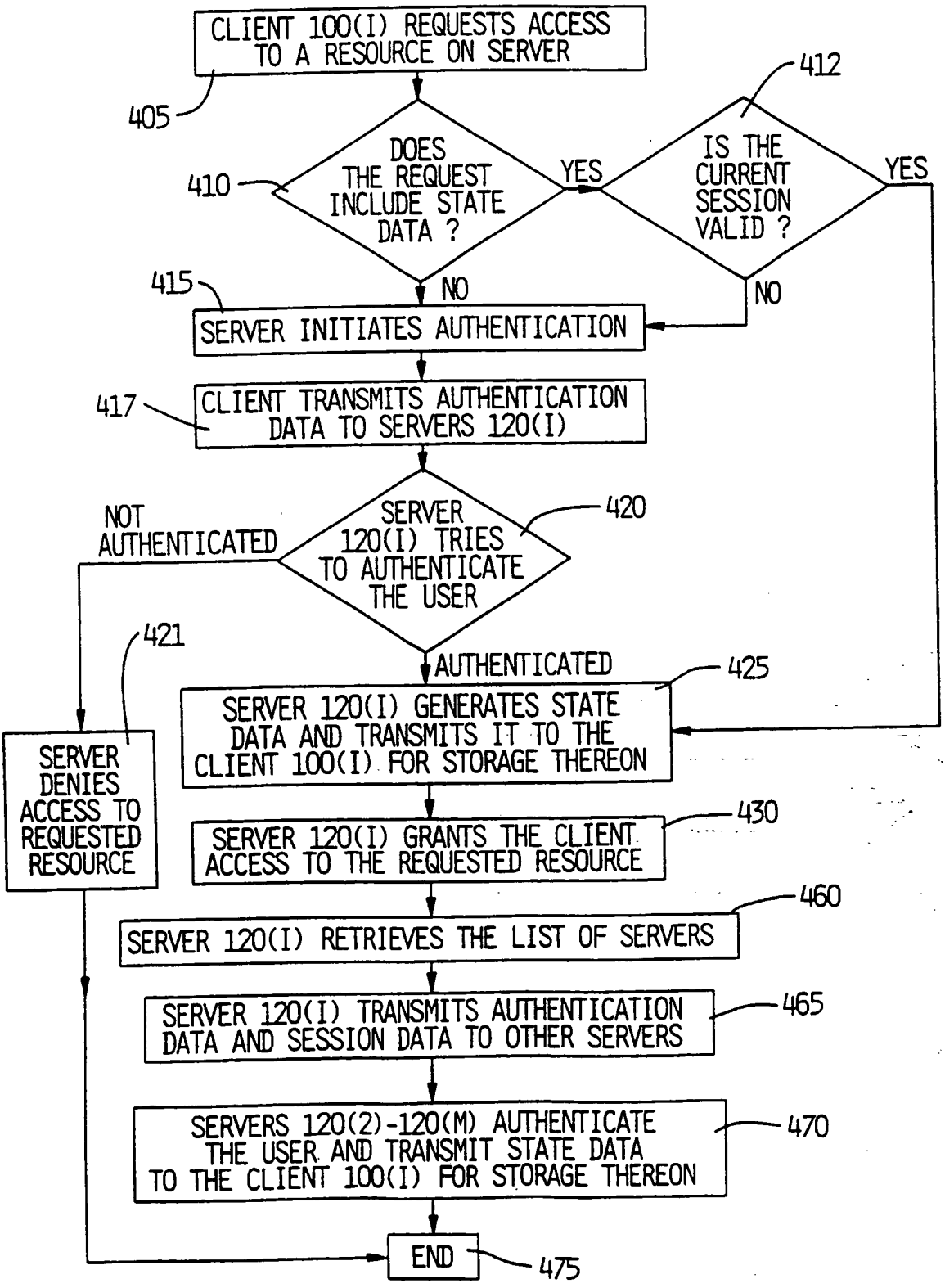

CLIENT 100(I) REQUESTS ACCESS TO A RESOURCE ON SERVER
350
DOES THE REQUEST INCLUDE STATE DATA ?
355
YES
NO
IS THE CURRENT SESSION VALID ?
357
YES
NO
360
SERVER INITIATES AUTHENTICATION
CLIENT TRANSMITS AUTHENTICATION DATA TO SERVERS 120(2)-120(M)
365
SERVERS 120(2)-120(M) AUTHENTICATE THE USER AND TRANSMIT STATE DATA TO THE CLIENT 100(I) FOR STORAGE THEREON
370
CLIENT 100(I) TRANSMITS AUTHENTICATION DATA TO SERVER 120(I)
375
SERVER 120(I) TRIES TO AUTHENTICATE THE USER
377
NOT AUTHENTICATED
AUTHENTICATED
380
SERVER 120(I) GENERATES STATE DATA AND TRANSMITS IT TO THE CLIENT 100(I) FOR STORAGE THEREON
SERVER DENIES ACCESS TO REQUESTED RESOURCE
358
SERVER 120(I) GRANTS THE CLIENT ACCESS TO THE REQUESTED RESOURCE
385
END
390

FIG_3

FIG_4


CLIENT 100(I) REQUESTS ACCESS TO A RESOURCE ON SERVER
405
DOES THE REQUEST INCLUDE STATE DATA ?
410
YES
IS THE CURRENT SESSION VALID ?
412
YES
NO
NO
415
SERVER INITIATES AUTHENTICATION
CLIENT TRANSMITS AUTHENTICATION DATA TO SERVERS 120(I)
417
SERVER 120(I) TRIES TO AUTHENTICATE THE USER
420
NOT AUTHENTICATED
AUTHENTICATED
421
SERVER DENIES ACCESS TO REQUESTED RESOURCE
SERVER 120(I) GENERATES STATE DATA AND TRANSMITS IT TO THE CLIENT 100(I) FOR STORAGE THEREON
425
SERVER 120(I) GRANTS THE CLIENT ACCESS TO THE REQUESTED RESOURCE
430
SERVER 120(I) RETRIEVES THE LIST OF SERVERS
460
SERVER 120(I) TRANSMITS AUTHENTICATION DATA AND SESSION DATA TO OTHER SERVERS
465
SERVERS 120(2)-120(M) AUTHENTICATE THE USER AND TRANSMIT STATE DATA TO THE CLIENT 100(I) FOR STORAGE THEREON
470
END
475

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00 | A3

(11) International Publication Number: WO 99/56194

(43) International Publication Date: 4 November 1999 (04.11.99)

(21) International Application Number: PCT/US99/09441

(22) International Filing Date: 29 April 1999 (29.04.99)

(30) Priority Data:

60/083,714	30 April 1998 (30.04.98)	US
09/283,540	1 April 1999 (01.04.99)	US

(71) Applicant: EC CUBED, INC. [US/US]; Suite 310, 15 River Road, Wilton, CT 06897 (US).

(72) Inventors: BARTOLOMEOS, Ephrem; 86 Grove Street #B6, Stamford, CT 06901 (US). WAINGANKAR, Pramod; 9 Hamilton Avenue, Norwalk, CT 06897 (US). RENGARAJAN, Vasu; 10 Clapboard Ridge Road #42J, Danbury, CT 06811 (US). HOQUE, Faisal; 96 Glenbrook Road #38, Stamford, CT 06902 (US).

(74) Agent: COHEN, Neil, G.; Cummings & Lockwood, Four Stamford Plaza, Stamford, CT 06904 (US).

(81) Designated States: CN, IN, JP, RU, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

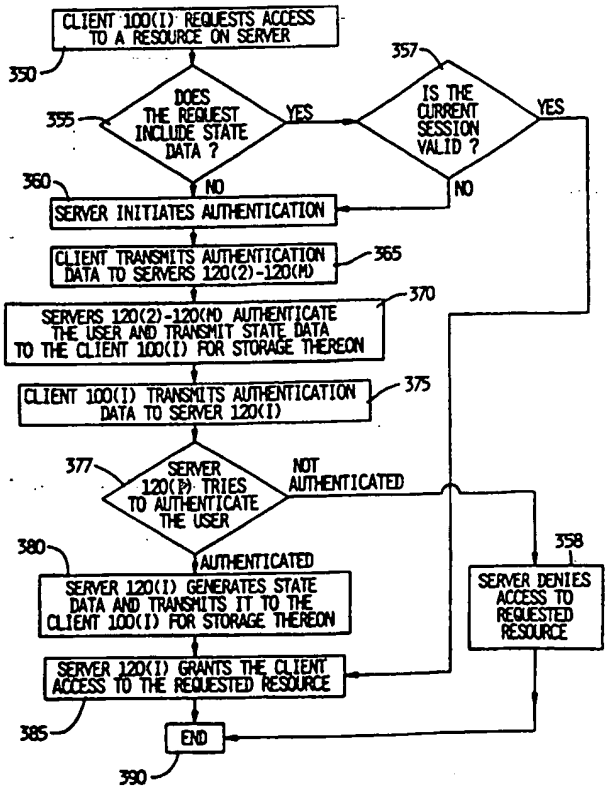
Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
13 January 2000 (13.01.00)

(54) Title: SYSTEM AND METHOD FOR AUTHENTICATING A USER TO MULTIPLE SERVERS IN A DISTRIBUTED COMPUTING NETWORK

(57) Abstract

A method and system for a server to facilitate authentication of a user of a client by a second server is disclosed. According to a disclosed method, the server, the second server, and the client communicate in a distributed computing network and the server and the second server store a plurality of restricted resources. The method includes the steps of storing data identifying the second server in the server, receiving a request to access one of the plurality of restricted resources from the client, and transmitting the data identifying the second server to the client so that the user of the client can be authenticated by the second server.



INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/US 99/09441

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 573 248 A (HUGHES AIRCRAFT COMPANY) 8 December 1993 (1993-12-08) column 1, line 1 -column 6, line 30; claims; figures	1-43
A	EP 0 773 489 A (I. B. M.) 14 May 1997 (1997-05-14) page 2, line 34 -page 4, line 35 page 5, line 49 -page 12, line 49; claims; figures 2-6	1-39
A	US 5 708 780 A (T. M. LEVERGOOD) 13 January 1998 (1998-01-13) column 3, line 5 -column 10, line 36; claims; figures 1-6	1,11,13, 21,29,31

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 November 1999	30/11/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Soler, J

1

Form PCT/ISA/210 (second sheet) (July 1992)